A Decoupled Blockchain Approach for Edge-envisioned IoT-based Healthcare Monitoring

Gagangeet Singh Aujla, *Senior Member, IEEE,* Anish Jindal, *Member, IEEE*

***Abstract*—The in-house health monitoring sensors form a large network of Internet of things (IoT) that continuously monitors and sends the data to the nearby devices or server. However, the connectivity of these IoT-based sensors with different entities leads to security loopholes wherein the adversary can exploit the vulnerabilities due to the openness of the data. This is a major concern especially in the healthcare sector where the change in data values from sensors can change the course of diagnosis which can cause severe health issues. Therefore, in order to prevent the data tempering and preserve the privacy of patients, we present a decoupled blockchain-based approach in the edge-envisioned ecosystem. This approach leverages the nearby edge devices to create the decoupled blocks in blockchain so as to securely transmit the healthcare data from sensors to the edge nodes. The edge nodes then transmit and store the data at the cloud using the incremental tensor-based scheme. This helps to reduce the data duplication of the huge amount of data transmitted in the large IoT healthcare network. The results show the effectiveness of the proposed approach in terms of the block preparation time, header generation time, tensor reduction ratio, and approximation error.**

***Index Terms*—Blockchain, Edge Computing, Healthcare, Internet of Things, In-home Monitoring.**

I. Introduction

THE Internet of things (IoT) has led to tremendous growth and development in a number of data-driven applications and services including transportation, networking, smart cities, and healthcare. Out of these, the healthcare sector has been the most sensitive and data critical service which relies on the continuous monitoring of patients' health through various types of sensors [1]. In this regard, the sensors deployed around patients' premises form a large in-house healthcare IoT monitoring network that senses and transmits the data from sensors to the nearby devices or servers. However, due to the round the clock connectivity of nodes in this IoT network, it is prone to various security issues such as eavesdropping and data manipulation [2], [3]. This poses serious security concerns in the healthcare sector as the data manipulation can result in the wrong diagnosis which can create life-threatening situations for the patients under observation.

To prevent these scenarios, we make use of the blockchain-based approach which helps to ensure that the data (which is being sent) by the sensors is in the original form. The blockchain technology forms the backbone of various crypto-currencies, the most famous one being the Bitcoin [4], [5]. It uses the distributed and public ledger system to record the transactions in the system and ensures data integrity by encrypting, validating and storing the transactions in a verifiable manner [6]. Apart from crypto-currencies, blockchain has been widely used by researchers for numerous data security related applications ranging from managing the financial transactions to providing secure energy trading [7], [8]. In the proposed secure in-house healthcare monitoring system, whenever a sensor sends the data, a unique block is created in the blockchain at a local edge node after validating the sensor's data. The use of edge node helps in a faster and much safer response from the IoT devices (i.e., sensors) and also manage control operations on the gathered data [9]. It is to be noted that each sensor would have a separate block at the edge node and the data from a particular sensor would be added to its own block only. This improves the transaction rate and moreover the transactions can be appended in the blockchain in a concurrent manner. The use of local edge nodes to store the blockchain results in very rapid data exchange as only a limited number of sensors are registered to each edge node. These edge nodes can be placed at urban heath premises or in primary health centers and are responsible for transmitting the data gathered from the sensors to the cloud server.

However, as the edge nodes have limited resources, therefore we use the decoupled blockchain-based approach where the block header and block ledgers are stored at different locations, and only the block headers are stored at the edge nodes. The concept of decoupled blockchain has been used in [10] for the smart vehicles to exchange their data in smart cities. The main premise behind the decoupling of blockchain is that one does not need the complete traditional block (in a blockchain) to validate the transaction and it can be decoupled into two entities known as block headers and block ledgers. Only the block header is enough for validating the identity of patients while appending transactions to the block of the patient while the block ledger (comprising of actual data), can be transmitted and stored at the cloud servers. More details on this are provided in Section III. This process ensures the identity verification (authentication), privacy and integrity of the data as well as prevents the data against the cyber-attacks.

Moreover, as edge nodes have limited resources and cater to the data generated by a large number of sensors, an efficient mechanism is required to limit the amount of data stored at the edge nodes. Most of the data gathered from these in-house health sensors would be same for the normal condition of the patients such as similar values of heart rate, blood pressure, etc. [11]. Therefore, one need not to store every data value generated from the sensors to reduce the amount of data stored

G. S. Aujla is with the School of Computing, Newcastle University, Newcastle Upon Tyne, United Kingdom (Email: gagi_aujla82@yahoo.com).

A. Jindal is with the School of Computer Science and Electronic Engineering, University of Essex, Colchester, United Kingdom (Email: anishjindal90@gmail.com).

at the edge node or cloud. For this purpose, an incremental tensor train decomposition approach has been used in this paper in order to prevent de-duplication at edge nodes as well as transmit the data in tensorized form so as to use optimal networking resources. This makes optimal use of underlying networking resources available in the large IoT healthcare network where the data could be accessed from anywhere by the concerned persons. The tensor data decomposition schemes have also been readily used by researchers for storing and transmitting data in various application domains such as transportation, smart grid, and IoT [12], [13].

A. Motivation

The security of the electronic health record of patients is of prime importance while sending data from an in-house healthcare monitoring system to the local or centralized controlled. This is because if an adversary is successfully able to gain access to this data, the privacy of the patients is jeopardized. Moreover, if this data is manipulated, it could lead to severe healthcare problems or wrong diagnosis which can, in the worst case, lead to patient's death. However, as the sensors have limited capacity, it is difficult to ensure safe and secure practices while transmitting the data. Therefore, a lightweight yet secure scheme is required which is able to provide data privacy while ensuring data integrity when communicating the data from in-house healthcare monitoring systems.

B. Contributions

The major contributions of the paper are listed as follows.

1) A generalized architecture for transmitting the in-house healthcare monitoring data to the cloud by leveraging edge nodes is presented.
2) A decoupled blockchain-based model is used for data security and privacy preservation in in-house healthcare monitoring ecosystem.
3) An incremental tensor train decomposition model is discussed in order to store the healthcare data at the cloud for preventing data duplication.

C. Organization

The rest of the paper is organized as follows. The related works are discussed in Section II while the system model is presented in Section III. The proposed schemes are elaborated in detail in Section IV and the results are discussed in Section V. Finally, the paper is concluded in Section VI.

II. Related work

Many researchers have leveraged the IoT networks for providing healthcare related solutions. Yin *et al.* [14] presented an overview of some of these IoT-based healthcare solutions. The authors highlighted the use of smart devices, resource management, and use of cloud computing and big data management related aspects to process the data gathered in heathcare IoT networks. To manage the resources in a smart healthcare framework in a better way, Oueida *et al.* [15] used the edge computing paradigm to model time independent resources. Rahmani *et al.* [16] also exploited the gateways at the edge of healthcare IoT networks to offload various tasks including local data storage and real-time data processing from cloud to edge gateways. The authors argued that such a scheme can be used to cater to different challenges in healthcare environment such as energy efficiency, scalability, and reliability. However, these edge gateways are prone to cyber-attacks which the authors had not considered.

One of the ways to ensure that the data transmitted from these edge devices to cloud is not tampered, is to use the concept of blockchain. Different researchers have used blockchain in different application areas to provide security in the underlying network. For instance, Jindal *et al.* [8] used edge-as-a-service for enabling energy trading in smart grid using blockchain-based transactions. Clauson *et al.* [17] have used blockchain in the healthcare systems to enhance the supply chain management to eliminate frauds or errors and increasing the trust in the supply chain process. Apart from this, blockchain has been widely used in healthcare networks for the purpose of access control, authentication, non-repudiation and interoperability. Recent surveys presented in [18], [19] sheds light on how the blockchain systems are being used by various healthacre researchers for achieving these security goals. In [19], the authors also highlight various challenges of using blockchain for processing the healthcare data, one of which is the issue of scalability. This issue arises when the resources at intermediary devices are limited while the number of service requests are constantly increasing. To cater to this issue, decoupled blockchain has been used in [10] where the authors stored block headers and block ledgers separately for smart city-based applications. This concept can be extended in the healthcare IoT networks to perform blockchain actions at the edge nodes.

Apart from this, another issue that arises in the healthcare IoT-based monitoring networks is data de-duplication. Most of the patient's sensory data, when in normal condition, is same and redundant; however, it is generally sensed, communicated, stored, and processed in the same manner as the critical data. To reduce the storage resources required by this data, various authors have used tensor-based data decomposition and storage techniques. For instance, He *et al.* [20] proposed a distributed, scalable, and sparse tensor factorization method to provide scalability and accuracy while performing healthcare analytics. Furthermore, Sandhu *et al.* [21] showed the applicability of tensor-based data representation and storage approach on the healthcare diabetes data. The authors noted that their tensor-based system provides faster computations, low latency, and high relevance as compared to the considered baseline models. The authors also highlighted that the cost of operation using this approach was reduced by 40% for running the queries to perform analytics on the data. All these schemes prove that tensor based approach to store and transmit healthcare monitoring data in IoT-based network could save networking resources and save associated operational costs.

III. System Model

The description of system model is provided in two parts, which are provided as below.

A. In-home Health Monitoring Model

The proposed in-home health monitoring model comprises of three layers, i.e., 1) IoT-Healthcare, 2) Edge-Blockchain, 3) Cloud layers. Fig. 1 depicts the three layered architecture of the proposed in-home health monitoring model.

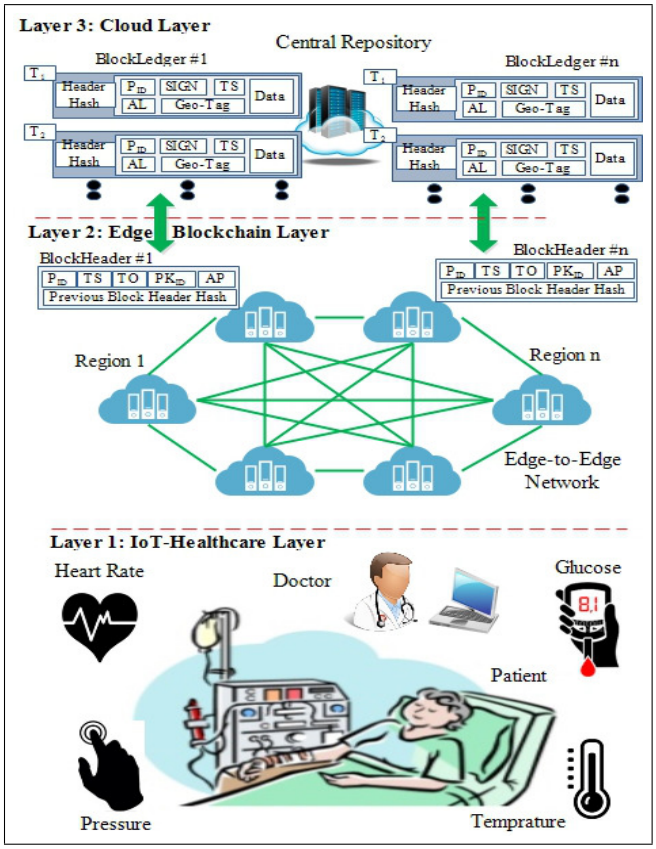


Fig. 1: System Model

The description of different layers is provided as below.

- *IoT-Healthcare layer:* This layer consists of *i* IoT-based healthcare monitoring devices and medical equipment's/implantable's (e.g., temperature sensors, heart rate devices, glucose monitor) which continuously gather vital heath parameters of the patient and transmit them to edge servers through gateway for processing and storage.
- *Edge-Blockchain layer:* Here, the edge devices or servers (*j*) located at primary or urban health centers across the geo-distributed locations form a peer to peer network. Each patient is registered to one edge node, which is responsible to collecting the associated patients data, process it, if required raise alarm in emergency situations, record the patients data, coordinate with cloud for backup. Each edge node can register multiple patients according to its resource availability. The edge ndoes are also responsible for authorising and validating the new transactions created by the patients and appending them to the block associated with each patient after consensus from peer edge nodes in the network. However, due to limited resource at edge nodes, a decoupled blockchain architecture has been adopted in the model which allows only block header to be stored at edge nodes and the block ledger comprising of entire data transactions are stored at the cloud layer (which has abundant computational and storage resources). The data in the block ledger is transmitted from edge to cloud in a tensorized format.
- *Cloud layer:* This layer is responsible to store the block ledger for each registered patient. For each patient, an incremental tensor train is maintained at cloud layer and the data send from the edge layer is appended to the tensor train in an incremental format. whenever required, the cloud layer transmits the data back to the edge.

B. Lightweight and Decoupled Blockchain Architecture

In this mechanism, each edge node participates in the blockchain for validation of the transactions created by geo-located patients and appending new blocks. Although there are many conventional blockchain frameworks like Bitcoin, IOTA, etc, but they have have some of the other implementation challenges. For example, Bitcoins requires high computing resources to run proof of work consensus mechanism [7] whereas IOTA end up in higher latency while adding new transactions [22]. Hence, such architectures are not suitable in a IoT-based in-home monitoring systems supported by edge computing. As the edge nodes and even the healthcare monitoring devices are equipped with limited computational and storage resources, so a novel lightweight permissioned blockchain mechanism inspired from [10] is designed. In this architecture, a single on-demand block per patient is created which is identified though its registered ID and public key. Each created block consists of electronic health record of the specific patient only. This allows the reduction in the time involved during waiting for the appending of other patients data transactions. Moreover, the patient side is responsible for collecting sensor data, signing it and generating a new transaction to be added in the block associated with the patient.

Each block consists of two components, 1) block header, and 2) block ledger. In this architecture, the edge nodes have to maintain only block header, which consists of only highly relevant information related to the registered patients. Moreover, the edges are responsible for signing the transactions which are related to the block header. The most important aspect of this architecture is that the hash of the header is of the previous block is the only portion which is included in the header of the next generated block. In this ways, a connection is created among the blocks appended in the blockchain. Also, the header must contain the necessary information which is required to verify whether the transactions have been generated by owner of the public key. The block header also included a time out field which contains a expiry time for public key in order to keep the freshness of the key. As the block data can be accessed by patients, doctors and other valid parties through there access control policies. So, each of these parties have different access levels which are appended in the block header as well as block ledger in the proposed mechanism.

Block ledger is responsible of storing the payload, i.e., the actual transactions associated with a specific patient. The transactions are stored at cloud data centers as shown in Fig.1 as the edge nodes have limited storage capacity. The edge

nodes validated the transactions as it can access the patients public key stored in the header of the block. Once validated, the transaction is appended to the existing block linked with that patient. The proposed architecture allows the addition of data in the block in parallel as all the transactions of a node are chained to the same block header. This makes processing faster and the decoupling of header and ledger among edge and cloud keeps the blockchain lightweight. Fig. 2 shows the structure of the decoupled blockchain adopted in this paper. Another salient feature of this architecture is the inclusion of geo-tag in the block ledger associated with the location of patient or sensor generating the vital data.

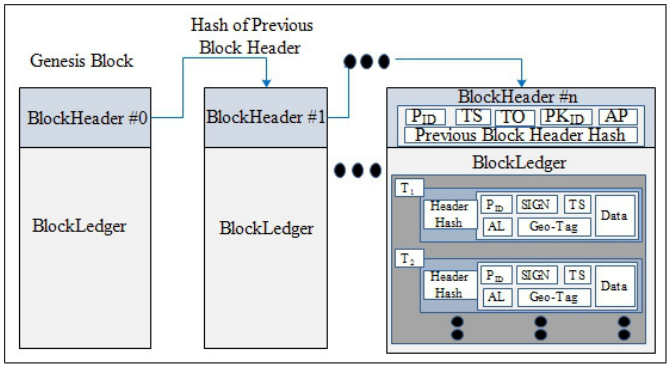


Fig. 2: Decoupled blockchain architecture

IV. The Proposed Scheme

The proposed edge-envisioned healthcare monitoring system consists of two sub parts, 1) Lightweight Blockchain Mechanism for in-home health monitoring, and 2) Incremental Tensor Decomposition for transmitting the patient data from edge to cloud. These two sub parts are described comprehensively in following sub-sections.

A. Lightweight Blockchain Mechanism

The proposed healthcare monitoring system is supported by a lightweight private blockchain mechanism which ensures data integrity and privacy preservation of patients and other participant in healthcare ecosystem. This mechanism is segregated into different phases described as below.

1) Registration or Initialization Phase: In this phase, $\mathbb{P}_i$ is registered with the available $\mathbb{E}_j$ using an approach based on the zero knowledge proof (ZKP) protocol [23]. This protocol is used to authenticate two parties without the exchange of secret information between them. Here, one party becomes the challenger (asks a query to the prover) and the other party is the prover (responds with the correct response). If the response of the prover is correct, it is said to be a verified party [24]. Here, $\mathbb{E}_j$ registers $\mathbb{P}_i$ which initiates a request ($\mathbb{R}_i$) after verification using ZKP. The steps involved in the one time registration and verification process are explained as below.

- In the first step, the registration process is initiated by generating a temporary key ($\mathbb{TK}_i$) which consists of three values, 1) temporary identity of the $\mathbb{P}_i$ ($\mathbb{T}_i^{\mathbb{ID}}$), 2) sensor identity ($\mathbb{S}_i^{\mathbb{ID}}$), and geographical location tag ($\mathbb{G}_i^{\mathbb{TAG}}$). It is pertinent to mention here that as the sensors connected to a patient may vary (number and type), so $\mathbb{S}_i^{\mathbb{ID}_k}$ comprises of *k* IDs associated to different healthcare sensors. Also, the MAC address of the sensors and other associated devices are also considered in $\mathbb{S}_i^{\mathbb{ID}_k}$. Now, the time stamp ($\mathbb{TS}_i$) of $\mathbb{TK}_i$ is recorded in a temporary store for tracking of the request generation sequence if required. After this, the $\mathbb{TK}_i$ is passed to $\mathbb{E}_j$ over secure channel.
- As $\mathbb{E}_j$ receives the $\mathbb{TK}_i$, it extracts its constituent attributes. Then, SALT-A, which is a pseudo random number is appended to $\mathbb{TK}_i$ in order to protect against pre-computed hash attack. SALT refers to random bits that are added to the data before it is hashed in order to create a unique value to prevent pre-computed hash attack. Now, the SALT-A and $\mathbb{TK}_i$ are concatenated and hashed using SHA-2. In this scheme, SHA-2 is used to create a 256 bit hash value because it is computationally inexpensive as compared to its later counterparts and cryptographically better in contrast to its former variants. After this, the hash ($\mathbb{H}[\mathbb{ID}]_j$) along with the public key of $\mathbb{E}_j$ ($\mathbb{PK}_j$) are passed to $\mathbb{P}_i$ over secure channel (SSL/TLS).
- Now, the *ZKP process* is initiated for *verification*. On receiving the information from $\mathbb{E}_j$, the $\mathbb{P}_i$ computes the SALT-A value. The brute force mechanism is used to find every possible combination of $\mathbb{TK}_i$ and SALT-A such that the output is equivalent to $\mathbb{H}[\mathbb{ID}]_j$. A new SALT-B is computed at patient end to increase the level of difficulty from patients end followed by the computation of a value (y). The value of y is based on a large prime number (p) and a generator (g). In this ZKP process, $\mathbb{P}_i$ is the prover and $\mathbb{E}_j$ is the verifier. $\mathbb{P}_i$ has to prove the knowledge of the $\mathbb{TS}_i$, such that $y = g^{\mathbb{TS}_i} mod\ p$. But, it cannot reveal the value of $\mathbb{TS}_i$ in the entire process. So, the entire process is focused on the knowledge of the value of $\mathbb{TS}_i$ without disclosing it to anyone. $\mathbb{P}_i$ computes a random value (r) which is used to further compute $d = g^r mod\, p$. The value of d which is used to generate $\mathbb{H}_i$ using the SALT-B is revealed to $\mathbb{E}_j$. Finally, the generated $\mathbb{H}_i$ is encrypted using $\mathbb{PK}_j$ to get an output as ZKP which is communicated to $\mathbb{E}_j$.
- After the receipt of ZKP, the $\mathbb{E}_j$ decrypts it using its secret key and extracts the value of $g^r mod\ p$ such that the hash of $g^r mod\, p$ and SALT-B is equivalent to ZKP. Now, $\mathbb{E}_j$ asks any of the two questions, i.e., Q $\rightarrow$ Q1 or Q2 with an equal probability, where $Q_1 = \mathbb{TS}_{i+\mathbb{R}}$ and $Q_2 = (\mathbb{TS}_i + \mathbb{TS}_{i+\mathbb{R}})\ mod(p-1)$. The either of the two questions are appended with SALT-B, hashed and transmitted to $\mathbb{P}_i$.
- On receiving the questions, $\mathbb{P}_i$ provides either of the answers, i.e., A $\rightarrow$ A1 or A2 with respect the the question asked. The answer is appended with SALT-B, hashed and sent to $\mathbb{E}_j$ for verification.
- In the final step, $\mathbb{E}_j$ verifies the value of the received answer. If the answer is verified, it assigns a permanent ID ($\mathbb{ID}_i$) to the $\mathbb{P}_i$ and broadcast $\mathbb{ID}_i$ to all the edge nodes of the blockchain network. The $\mathbb{ID}_i$ is linked to the public key of $\mathbb{P}_i$. Whenever the time out occurs and a new public key is generated, it is again tagged to $\mathbb{ID}_i$

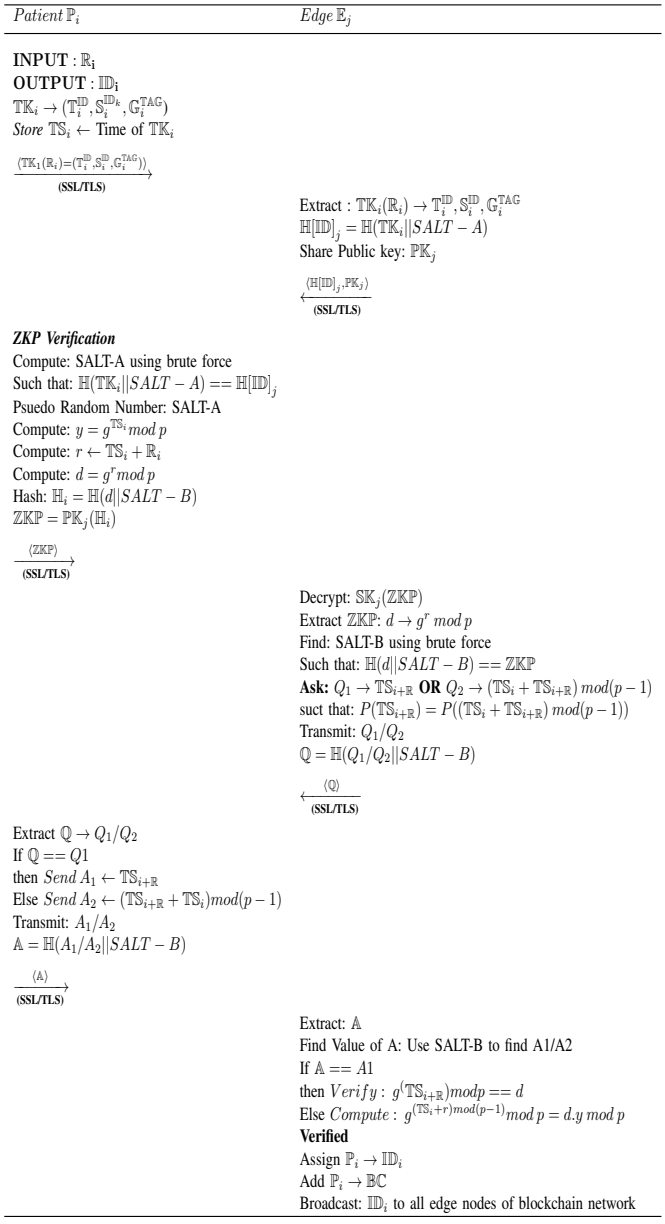


Fig. 3: Registration and Verification Phases

of the said patient.

Fig. 3 depicts the dialogue between $\mathbb{P}_i$ and $\mathbb{E}_j$ for the registration and verification process.

2) Block Creation and Validation Phase: In this phase, the block creation and validation process is described. Once the $\mathbb{P}_i$ have registered with a legitimate $\mathbb{E}_j$, it proceeds with the one time process to join the blockchain. The steps involved between $\mathbb{P}_i$, $\mathbb{E}_j$ and edge peers are described as below.

- In the first step, $\mathbb{P}_i$ generates a key pair $(\mathbb{PBK}_i, \mathbb{PRK}_i)$, where $\mathbb{PBK}_i$ is the public key and $\mathbb{PRK}_i$ represents the private key of i^{th} patient. Now, a key time out value $(\mathbb{TO}_i)$ is set which is used as a validity of the key pair. After $\mathbb{TO}_i$ expires, a new key pair has to be generates and the old key pair will not remain valid for all member nodes of the blockchain. After this, the process of edge discovery is initiated.
- Now, after the associated $\mathbb{E}_j$ is discovered, it generates its signature $(SIGN_j)$ and send it to $\mathbb{P}_i$ for validation.
- The received signature is validated by the $\mathbb{P}_i$ for verification purpose. If $SIGN_j$ is valid, $\mathbb{P}_i$ asks $\mathbb{E}_j$ for joining the blockchain using its $\mathbb{PBK}_i$, $\mathbb{G}_i^{\mathbb{TAG}}$, and $\mathbb{ID}_i$.
- On receipt, the $\mathbb{E}_j$ sends $\mathbb{G}_i^{\mathbb{TAG}}$ to the peer edge nodes for location validation.
- The edge peers in the network validates the location of the $\mathbb{P}_i$ though voting process and send back the status as T/F, i.e., true or false.
- If status is T, a new block $(\mathbb{B}_i)$ is generated and appended to the blockchain with respect to $\mathbb{PBK}_i$ and $\mathbb{ID}_i$.

The entire process of block creation and validation is summarized in the Fig. 4.

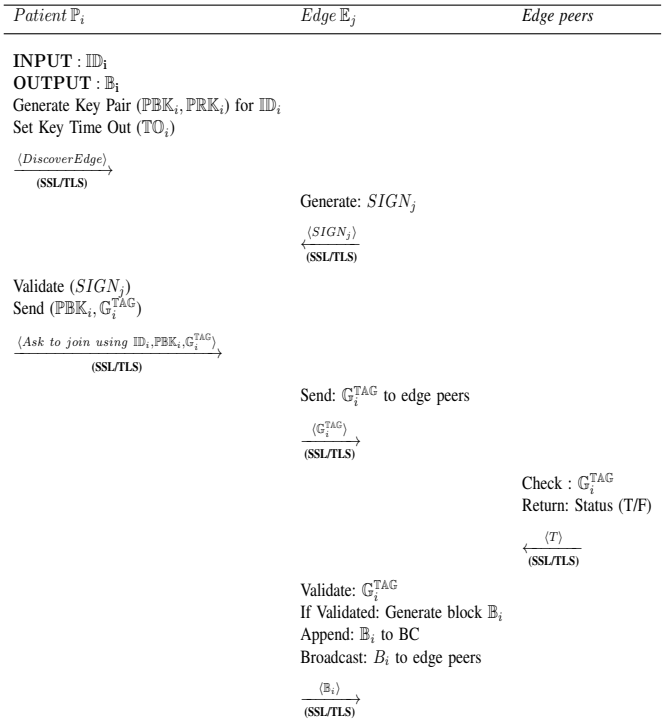


Fig. 4: Block creation and validation process

3) Data Generation and Block Updation Phase: In this phase, the process of data generation from different IoT/healthcare sensors attached to $\mathbb{P}_i$, transaction $(\mathbb{T}_i)$ creation and block updation takes place. The steps involved in this process are comprehensively described as below.

- In the first step, the data $(\mathbb{D}_i)$ generated from $\mathbb{S}_i^{\mathbb{ID}_k}$ is read and signed $(SIGN_i)$ using the $\mathbb{PRK}_i$ of $\mathbb{P}_i$. Once $\mathbb{D}_i$ has been signed, a new transaction $(\mathbb{T}_i)$ comprising of $\mathbb{D}_i$ along with the signature, $\mathbb{PBK}_i$ and $\mathbb{ID}_i$ of the patient is created. Now, $\mathbb{T}_i$ is sent to $\mathbb{E}_j$ for validation and thereafter updation in $\mathbb{B}_i$.
- Now, a valid record for the received $\mathbb{PBK}_i$ and $\mathbb{ID}_i$ in blockchain is searched. If a valid entry is found in the blockchain, the $\mathbb{D}_i$ and $SIGN_i$ are checked and validated. If all the validations are complete, the $\mathbb{T}_i$ is appended to $\mathbb{B}_i$ and the updated $\mathbb{B}_i$ is broadcast to the entire blockchain.

- On receipt of the updated $\mathbb{B}_i$, the entire blockchain is synchronized.

The dialogue for the data generation and block updation phases is presented in the Fig. 5.

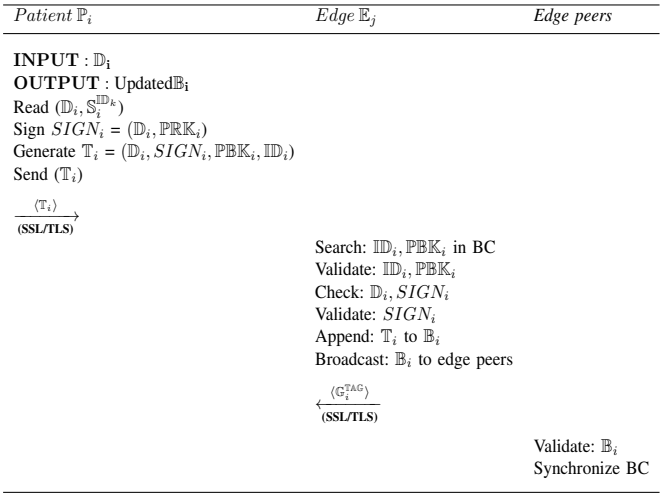


Fig. 5: Data generation and block updation process

B. Incremental Tensor Train Decomposition

In this section, the incremental tensor train decomposition scheme for dimensionality reduction is presented. This scheme helps to remove the unwanted attributes or dimensions of the high dimensional data generated by healthcare sensors, thereby extracting a compact form of data which not only reduces storage space but also relieves the load of the underlying network during transmission. Although different tensor representations have been adopted in the literature [12], [13], [25], but they have there own limitations when the the tensor's order reaches to thousands. As the volume of the tensor increase so does the additional overhead due to different tensor operations and computations. So, to tackle such a situation, the tensor train is a simplistic tensor network format which is based on low-rank approximation of auxiliary unfolding matrix. It is very balanced approach to handle the high-order tensors and can support different different algebraic operations.

Now, one of the major problem in the healthcare patient data is that the data is being continuously generated (dynamic) and hence it is very difficult to append the newly generated generated data to the original tensor. Moreover, it is not possible to reconstruct the tensor after decomposition and then update it to obtain a new tensor due to the higher order of dimentionality. Also, the real analysis of patients health statistics and vital parameters required lower delay which mean lower decomposition time. All the above listed challenges can be effectively handles using an incremental approach in integration with the tensor train format used in [25]. Hence, the data generated from sensors is converted into a tensor-based representation and thereafter added to a tensor train network which further follows the incremental process to prevent the repeated decomposition of the older data.

Basically, an n^{th} order tensor (T) is represented as below.

$$T \in R^{I_1, I_2, I_3, \cdots, I_n} \tag{1}$$

where, I (1 to n) represents the dimensions of the data.

Now, the tensor train format for an n^{th} order tensor, i.e., $T \in R^{I_1, I_2, I_3, \cdots, I_n}$ is represented as follows.

$$T = T^{(1)} \bigotimes T^{(2)} \bigotimes T^{(3)} \cdots \bigotimes T^{(k)} \bigotimes \cdots \bigotimes T^{(n)} \tag{2}$$

where, $T^{(k)} \in R^{(k) \times I_k \times r_k}$, s.t., $k = (1, \cdots n)$ and $r_0 = r_n = 1$ is known as core tensors, $r_0, r_2, \cdots, r_n$ represents the ranks for tensor train format, and $\bigotimes$ denotes contraction dot product.

Based on a series of Singular Value Decomposition's (SVDs) of auxiliary unfolding matrices [13], the tensor train decomposition relies completely on low-rank decomposition. As such, the decomposition of n^{th} order tensor based on tensor train concept have to follow *n-1* sequential SVDs. For each of the SVD, the left singular matrix is converted into current core tensor and the remaining part is executed using SVD till the final core tensor is extracted. For a given unfolding matrix (M), if the singular values are shortened at γ as follows:

$$||\mathbb{M} - \hat{\mathbb{M}}||_{\mathbf{F}} \leq \gamma ||\mathbb{M}||_{\mathbf{F}} \tag{3}$$

where, $\hat{\mathbb{M}}$ is the reconstructed matrix and γ denoted the threshold value equivalent to the rank.

Now, the approximation error (prescribed accuracy) between T and approximate tensor ($\hat{T}$) is given as below.

$$e = \sqrt{n-1}\gamma \tag{4}$$

The above expression can be expanded as shown below.

$$||T - \hat{T}||_{\mathbf{F}} \leq e||T||_{\mathbf{F}} \tag{5}$$

The Algorithm 1 is presented to depict the tensor train decomposition for an n^{th} order tensor. In this algorithm, the prescribed accuracy is initialized, T is defined as temporary tensor X, and r_0 is set to 1. The the unfolding process is used to SVD to get two singular matrices (U,V) and a diagonal matrix (S). Following the process defined in [26], the tensor cores are extracted.

Algorithm 1 Tensor train decomposition

Input: $T \in R^{I_1, I_2, I_3, \cdots, I_n}$
Output: $T = T^{(1)} \bigotimes T^{(2)} \bigotimes T^{(3)} \bigotimes \cdots \bigotimes T^{(n)}$

INITIALIZE: $\gamma = \frac{e}{\sqrt{n-1}}||T||_{\mathbf{F}}$, $X \leftarrow T$, $r_0 == 1$
for ($k \leftarrow 1$ to $n-1; k \leq n; k++$) **do**
  $M \leftarrow Unfolding - k(X[r_{k-1}, I_k, \frac{M}{r_{k-1}, I_k}])$
  [U,S,V] $\leftarrow$ SVD(M, γ)
  $M = USV^T$
  $\gamma_k \leftarrow rank_\gamma(M)$
  $T^(k) \leftarrow Tensorization(U, [r_{k-1}, I_k, r_k])$
  $X \leftarrow SV^T$
end for
$T^{(n)} \leftarrow Tensorization(T, [r_{n-1}, I_n, r_n])$
$r_n \leftarrow 1$
RETURN cores $T^{(1)} \bigotimes T^{(2)} \bigotimes T^{(3)} \bigotimes \cdots \bigotimes T^{(n)}$

Now, after the computation of tensor train format of X, the incremental tensor train decomposition process is initiated. Initially, the temporary tensor *X* and incremental tensor *Y* are converted into tensor train format using Algorithm 1. After this, zeroes are added to *X* and *Y* to convert them into

zero padded tensor train format, i.e., $X^{'}$ and $Y^{'}$ according to the rules of yielding all new tensor-train cores $X'^{(k)}(i_k)$ are defined as below [25], [26].

$$X'^{(k)}(i_k) = \begin{cases} 0, & k = m \ and \ i_k > I_m; \\ X^{(k)}(i_k), & otherwise \end{cases} \quad (6)$$

After the zero padding process, the $X^{'}$ and $Y^{'}$ are merged to achieve consistency and remove duplicate cores. The merged tensor train cores are represented as follows [25].

$$Z'(i_1, i_2, .., i_n) \Rightarrow X'(i_1, i_2 \cdots, i_n) + Y'(i_1, i_2 \cdots, i_n) \quad (7)$$

Algorithm 2 depicts the incremental tensor train decomposition similar to [12], [25].

Algorithm 2 Incremental tensor train decomposition

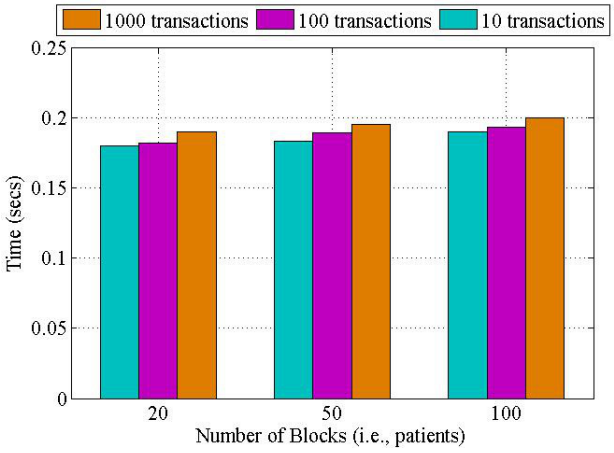
Input: $T \in R^{I_1,I_2,I_3,\cdots,I_k,\cdots,I_n}$, $T \in Y^{I_1,I_2,I_3,\cdots,I_k^{'},\cdots,I_n}$
Output: Tensor train cores, $Z^{(1)}, Z^{(2)}, Z^{(3)}, \cdots, Z^{(n)}$

TENSOR TRAIN FORMAT ← Y (Follow Algorithm 1)
$Y_{TT}(Y^{(1)}, Y^{(2)}, Y^{(3)}, \cdots, Y^{(n)})$ ← TT(Y,e)
ZERO PADDING ← X, Y (Follow Eq. 6)
$X^{'}_{TT}(X^{'(1)}, X^{'(2)}, \cdots, X^{'(n)})$ ← TT-zeroes(X_{TT}, k)
$Y^{'}_{TT}(Y^{'(1)}, Y^{'(2)}, \cdots, Y^{'(n)})$ ← TT-zeroes(Y_{TT},k)
ADDITION ← $X^{'}$, $Y^{'}$ (Follow Eq. 7)
$Z^{'}_{TT}(Z^{'(1)}, Z^{'(2)}, \cdots, Z^{'(n)})$ ← ADD-TT($X^{'}_{TT}$, $Y^{'}_{TT}$)
if (OR == SATISFIED) **then**
    BEGIN(OR PROCESS)
    $Z^{(1)}, Z^{(2)}, Z^{(3)}, \cdots, Z^{(n)}$ ← ORTH-TT($Z^{'}_{TT}$,e)
    Compute Truncation Parameter: $\gamma = \frac{e}{\sqrt{n-1}}$
    for (k ← n to 2) **do**
        M_k ← RESHAPE ($Z^{(k)}, [r_{k-1}, I_k * r_k]$)
        [Q,R] ← QR(M_k)
        $Z^{(k)}$ ← RESHAPE ($Q, [r^{'}_{k-1}, I_k, r_k]$)
        $Z^{(n-1)}$ ← $Z^{(n-1)} \times_3$ R
    end for
end if
if (e ≠ o) **then**
    for (k ← 1 to n-1) **do**
        M_k ← RESHAPE ($Z^{(k)}, [r_{k-1} * I_k, r_k]$)
        [U,S,V] ← SVD(M, γ)
        [Q,R] ← QR(M_k)
        $Z^{'(k)}$ ← RESHAPE ($U, [r_{k-1}, I_k, r^{'}_k]$)
        $Z^{(n+1)}$ ← $Z^{(n+1)} \times_1 SV^T$
    end for
end if
RETURN $Z^{(1)}, Z^{(2)}, Z^{(3)}, \cdots, Z^{(n)}$

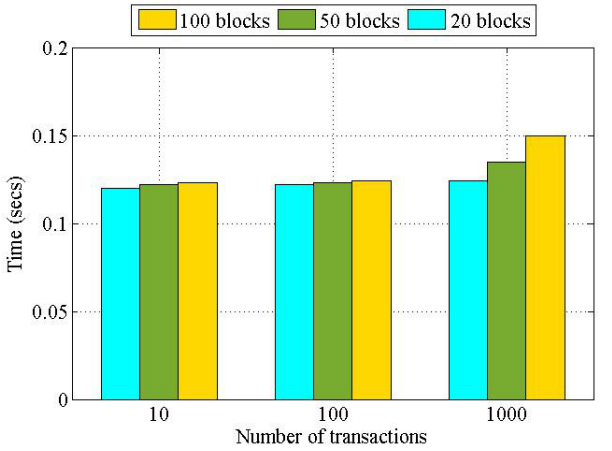
V. Results and Discussions

To show the working of the proposed scheme for IoT-based healthcare monitoring systems, we use the MHEALTH dataset [27] (scaled up to 10 times). This dataset comprises 23 signals gathered from different sensors including accelerometer, electrocardiograms, gyroscope, and magnetometer placed on the person's chest, right wrist, and left ankle. The number of transactions generated by the patients which are appended to the individual blocks are considered in three groups, i.e., 10, 100, 1000. Even more, the number of patients are also varied in three scenarios, i.e., 20, 50, 100.

The initial evaluation of the proposed scheme involves the time consumed for the addition of a new block to the blockchain after it has registered using ZKP protocol [23]. This time includes the time related to the patients request to add the block, validation by edge node, addition of the block and updating the peers regarding the new block. The time taken to register using ZKP protocol has not been considered in this evaluation as it consumes almost equal time for all patients. Fig. 6(a) shows variation of time taken to add a block in the blockchain with respect to the number of patients (blocks). The time consumed, as depicted in Fig. 6(b), shows the increase in the processing time with respect to an increase in the number of transactions. It is clear that the time increases with an increase in the number of blocks as well as the number of transactions. The major reason for this increase is the time consumed for more number of validations performed by edge nodes.



(a) Block preparation time.



(b) Header generation time.

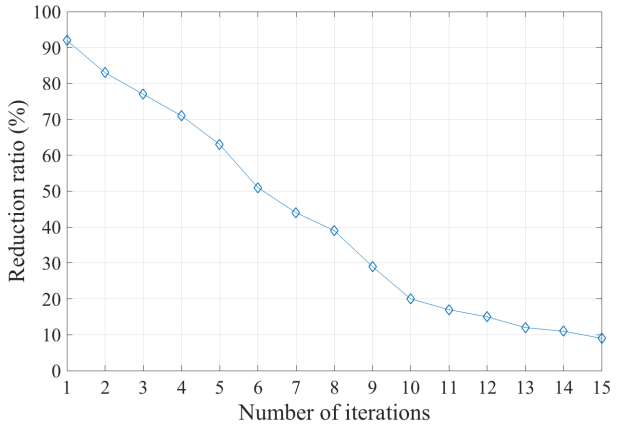
Fig. 6: Performance evaluation for blockchain-based scheme.

To check the performance of the proposed incremental tensor train decomposition algorithm on the considered dataset, two evaluation metrics are considered, viz. dimensionality reduction ratio and approximation error. The approximation

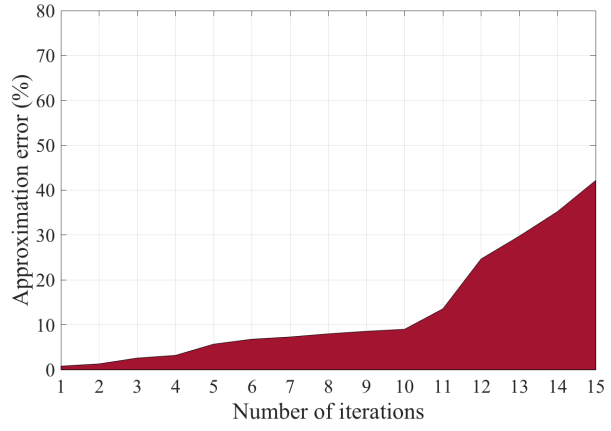
error is computed as given in Eq. 5, while the dimensionality reduction (ρ) is defined as the ratio of the non-zero values in the reduced tensor and orthogonal vectors to the non-zero values in the initial tensor. It is mathematically represented as,

$$\rho = \frac{nz(\hat{T}) + \sum_{i=1}^{n}(U_i)}{nz(T)} \tag{8}$$

Fig. 7(a) shows the dimensionality reduction ratio over number of iterations of algorithm 2. This figure shows that the reduction ratio increases with each iteration, however, considering the approximation error in Fig. 7(b), it is best to stop the algorithm at 10 iterations to have a better reduction ratio and approximation error trade-off. At tenth iteration, approximately 20% of the data values gives the approximation error of 9%. Therefore, the tensor values at tenth iteration are sent over from edge device to the cloud storage. This saves a lot of storage resources at the cloud while re-constructing the patients' data without much error. For this case, it means that only 20% of the core tensor data values are able to reconstruct the complete data with 91% accuracy. Moreover, the communication resources required to send the reduced tensor to the cloud are also decreased as compared to the scenario where the full data was to be sent.



(a) Reduction ratio.



(b) Approximation error.

Fig. 7: Results obtained for incremental tensor train approach.

VI. Conclusion

The proposed approach provides a fast and efficient way to communicate the in-house IoT healthcare data to the edge devices. This approach uses decoupled blockchain-based scheme to bifurcate the block headers and ledgers which reduce the block preparation and header generation times while preserving the security while communicating the gathered data. To further send the data from edge devices to the cloud server, an incremental tensor train scheme has been used which reduces the overall storage space at the cloud while re-considering the same data with very less error. The results in terms of blockchain and tensor based evaluation metrics prove the effectiveness of the proposed approach.

In future, we will test the use of advance communication technologies such as 5G, software defined networks, etc. to improve the performance of underlying network services.

References

[1] A. Jindal, A. Dua, N. Kumar, A. V. Vasilakos, and J. J. Rodrigues, "An efficient fuzzy rule-based big data analytics scheme for providing healthcare-as-a-service," in *2017 IEEE International Conference on Communications (ICC)*. IEEE, 2017, pp. 1–6.

[2] I. Stellios, P. Kotzanikolaou, M. Psarakis, C. Alcaraz, and J. Lopez, "A survey of iot-enabled cyberattacks: Assessing attack paths to critical infrastructures and services," *IEEE Communications Surveys Tutorials*, vol. 20, no. 4, pp. 3453–3495, Fourthquarter 2018.

[3] A. Burg, A. Chattopadhyay, and K. Lam, "Wireless communication and security issues for cyber–physical systems and the internet-of-things," *Proceedings of the IEEE*, vol. 106, no. 1, pp. 38–60, Jan 2018.

[4] L. R. Abbade, F. M. Ribeiro, M. H. da Silva, A. F. Morais, E. S. de Morais, E. M. Lopes, A. M. Alberti, and J. J. Rodrigues, "Blockchain applied to vehicular odometers," *IEEE Network*, vol. 34, no. 1, pp. 62–68, 2020.

[5] S. Saha, A. K. Sutrala, A. K. Das, N. Kumar, and J. J. P. C. Rodrigues, "On the design of blockchain-based access control protocol for iot-enabled healthcare applications," 2020.

[6] Z. Zheng, S. Xie, H.-N. Dai, X. Chen, and H. Wang, "Blockchain challenges and opportunities: A survey," *International Journal of Web and Grid Services*, vol. 14, no. 4, pp. 352–375, 2018.

[7] S. Aggarwal, R. Chaudhary, G. S. Aujla, N. Kumar, K.-K. R. Choo, and A. Y. Zomaya, "Blockchain for smart communities: Applications, challenges and opportunities," *Journal of Network and Computer Applications*, vol. 144, pp. 13 – 48, 2019.

[8] A. Jindal, G. S. Aujla, and N. Kumar, "Survivor: A blockchain based edge-as-a-service framework for secure energy trading in sdn-enabled vehicle-to-grid environment," *Computer Networks*, vol. 153, pp. 36–48, 2019.

[9] M. W. Condry and C. B. Nelson, "Using smart edge iot devices for safer, rapid response with industry iot control operations," *Proceedings of the IEEE*, vol. 104, no. 5, pp. 938–946, May 2016.

[10] R. A. Michelin, A. Dorri, M. Steger, R. C. Lunardi, S. S. Kanhere, R. Jurdak, and A. F. Zorzo, "Speedychain: A framework for decoupling data from blockchain for smart cities," in *Proceedings of the 15th EAI International Conference on Mobile and Ubiquitous Systems: Computing, Networking and Services*. ACM, 2018, pp. 145–154.

[11] A. Ullah, I. Sehr, M. Akbar, and H. Ning, "Fog assisted secure de-duplicated data dissemination in smart healthcare iot," in *IEEE International Conference on Smart Internet of Things*, 2018, pp. 166–171.

[12] A. Singh, G. S. Aujla, S. Garg, G. Kaddoum, and G. Singh, "Deep learning-based sdn model for internet of things: An incremental tensor train approach," *IEEE Internet of Things Journal*, 2019.

[13] D. Kaur, G. S. Aujla, N. Kumar, A. Y. Zomaya, C. Perera, and R. Ranjan, "Tensor-based big data management scheme for dimensionality reduction problem in smart grid systems: Sdn perspective," *IEEE Transactions on Knowledge and Data Engineering*, vol. 30, no. 10, pp. 1985–1998, Oct 2018.

[14] Y. Yuehong, Y. Zeng, X. Chen, and Y. Fan, "The internet of things in healthcare: An overview," *Journal of Industrial Information Integration*, vol. 1, pp. 3–13, 2016.

[15] S. Oueida, Y. Kotb, M. Aloqaily, Y. Jararweh, and T. Baker, "An edge computing based smart healthcare framework for resource management," *Sensors*, vol. 18, no. 12, p. 4307, 2018.

[16] A. M. Rahmani, T. N. Gia, B. Negash, A. Anzanpour, I. Azimi, M. Jiang, and P. Liljeberg, "Exploiting smart e-health gateways at the edge of healthcare internet-of-things: A fog computing approach," *Future Generation Computer Systems*, vol. 78, pp. 641–658, 2018.

[17] K. A. Clauson, E. A. Breeden, C. Davidson, and T. K. Mackey, "Leveraging blockchain technology to enhance supply chain management in healthcare," *Blockchain in Healthcare Today*, 2018.

[18] M. Hölbl, M. Kompara, A. Kamišalić, and L. Nemec Zlatolas, "A systematic review of the use of blockchain in healthcare," *Symmetry*, vol. 10, no. 10, p. 470, 2018.

[19] T. McGhin, K.-K. R. Choo, C. Z. Liu, and D. He, "Blockchain in healthcare applications: Research challenges and opportunities," *Journal of Network and Computer Applications*, 2019.

[20] H. He, J. Henderson, and J. C. Ho, "Distributed tensor decomposition for large scale health analytics," in *The World Wide Web Conference*. ACM, 2019, pp. 659–669.

[21] R. Sandhu, N. Kaur, S. K. Sood, and R. Buyya, "Tdrm: tensor-based data representation and mining for healthcare data in cloud computing environments," *The Journal of Supercomputing*, vol. 74, no. 2, pp. 592–614, 2018.

[22] G. S. Aujla, M. Singh, A. Bose, N. Kumar, G. Han, and R. Buyya, "Blocksdn: Blockchain-as-a-service for software defined networking in smart city applications," *IEEE Network*, vol. 34, no. 2, pp. 83–91, 2020.

[23] U. Feige, A. Fiat, and A. Shamir, "Zero-knowledge proofs of identity," *Journal of cryptology*, vol. 1, no. 2, pp. 77–94, 1988.

[24] G. S. Aujla, A. Singh, M. Singh, S. Sharma, N. Kumar, and K. R. Choo, "Blocked: Blockchain-based secure data processing framework in edge envisioned v2x environment," *IEEE Transactions on Vehicular Technology*, 2020.

[25] H. Liu, L. T. Yang, Y. Guo, X. Xie, and J. Ma, "An incremental tensor-train decomposition for cyber-physical-social big data," *IEEE Transactions on Big Data*, pp. 1–1, 2018.

[26] I. V. Oseledets, "Tensor-train decomposition," *SIAM Journal on Scientific Computing*, vol. 33, no. 5, pp. 2295–2317, 2011.

[27] O. Banos, R. Garcia, J. A. Holgado-Terriza, M. Damas, H. Pomares, I. Rojas, A. Saez, and C. Villalonga, "mhealthdroid: a novel framework for agile development of mobile health applications," in *Proceedings of the 6th International Work-conference on Ambient Assisted Living an Active Ageing (IWAAL 2014)*. Springer, 2014, pp. 91–98.

Gagangeet Singh Aujla (S'15, M'18, SM'19) received his Ph.D. in Computer Science and Engineering from Thapar Institute of Engineering and Technology, Patiala, Punjab, India in 2018. He received the B.Tech and M.Tech. degrees in Computer Science and Engineering from Punjab Technical University, Jalandhar, Punjab, India, in 2003 and 2013, respectively. Currently, he is working as an Post Doctorate Research Associate in the School of Computing, Newcastle University, Newcastle Upon Tyne, United Kingdom. He is also working as an Associate Professor in Computer Science and Engineering Department, Chandigarh University, Mohali, Punjab, India. Prior to this, he was working as a Research Associate in Indo-Austria Research project sponsored by Department of Science and Technology, Government of India and Ministry of Science, Austria. He is recipient of 2018 IEEE TCSC Award of Excellence for Outstanding Ph.D Dissertation at Guangzhou China. He has many research contributions in the area of smart grid, cloud computing, edge computing, vehicular networks, software defined networks, security and cryptography. He is on the Editorial Board of the Sensors Journal. He has been the Guest Editor for Special Issues in the IEEE Transactions on Industrial Informatics, the IEEE Network, Computer Communications (Elsevier), Software: Practice and Experience (Wiley), Transactions on Emerging Telecommunications Technologies (Wiley), and Security & Privacy (Wiley). He has been the Workshop Chair for various conferences including IEEE Infocom (2020), IEEE Globecom (2018), IEEE ICC (2019-20) and IEEE PiCom (2019-20). He is the Senior Member of the IEEE and Member of the ACM.

Anish Jindal (M'16, SM'17) is working as a Lecturer in School of Computer Science and Electronic Engineering (CSEE), University of Essex since Mar 2020. Prior to this, he worked as senior research associate at School of Computing & Communications, Lancaster University, UK from Oct. 2018 to Mar. 2020. He completed his Ph.D., M.E. and B. Tech. degrees in computer science engineering in 2018, 2014, and 2012, respectively. He is the recipient of the Outstanding Ph.D. Dissertation Award, 2019 from IEEE Technical Committee on Scalable Computing (TCSC) and conferred with the IEEE Communication Society's Outstanding Young Researcher Award for the Europe, Middle East, and Africa (EMEA) Region, 2019. He has served as General co-chair, TPC co-chair, TPC member, Publicity chair and Session chair of various reputed conferences and workshops including IEEE ICC, IEEE WoWMoM, IEEE INFOCOM and IEEE GLOBECOM. He is also the guest editor of various journals including Software: Practice and Experience (Wiley) and Computers (MDPI). His research interests are in the areas of smart cities, data analytics, artificial intelligence, cyber-physical systems, wireless networks, and security. He is a member of the IEEE and actively involved with various working groups and committees of IEEE and ACM related to smart grid, energy informatics and smart cities.